UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA

MARIANN ARCHER **and** **PATRICK REDDY** ***On behalf of herself and those similarly situated,*** **Plaintiffs,** vs. **OVERBY-SEAWELL CO.** **and** **KEYBANK, N.A.** **Defendants.**	**Case No.** **<u>CLASS ACTION COMPLAINT</u>** **JURY TRIAL DEMANDED**

Plaintiffs Mariann Archer ("Archer") and Patrick Reddy ("Reddy") (collectively, "Plaintiffs"), individually and on behalf of all those similarly situated (the "Class" or "Class Members"), bring this Class Action Complaint ("Complaint") against Defendant Overby-Seawell Co ("OSC") and Defendant KeyBank NA ("KeyBank") (collectively "Defendants") and make the following allegations upon their personal knowledge as to their own actions and their counsels' investigation, and upon information and belief as to all other matters, and that facts that are a matter

of public record.

INTRODUCTION

1. This class action stems from Defendants' failure to secure the sensitive personal information of their current and former customers and other consumers for whom Defendants performed services. KeyBank is the 24th largest bank is the United States. OSC provided KeyBank services including ongoing verification that KeyBank's residential mortgage customers maintain property insurance.

2. Plaintiffs bring this class action against Defendants for their failure to properly secure and safeguard sensitive personally identifiable information provided by and belonging to their customers, including, without limitation, names, mortgage property addresses, mortgage account numbers, mortgage account information, telephone numbers, property loan numbers, Social Security numbers, home insurance policy numbers, home insurance information, and additional personally identifiable information provided by and belonging to KeyBank customers in connection with a loan application, loan modification, or other items regarding loan servicing that Defendants collects and maintains ("PII" or "Sensitive Information").[1]

[1] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual.

3. In furtherance of services OSC performs on KeyBank's behalf, OSC obtains vast quantities of PII belonging to KeyBank's customers, including Plaintiffs and Class Members.

4. This class action arises out of the recent targeted cyberattack against OSC that, by Defendants' own admission, allowed unauthorized third-party intruders to remotely access OSC's computer systems and data, resulting in the exfiltration of highly sensitive PII belonging to thousands of current and former KeyBank clients (the "Data Breach").

5. Because of the Data Breach, Plaintiffs, and thousands of other victims ("Class Members"), suffered ascertainable losses in the form of the loss of the benefit of their bargain, out-of-pocket expenses, and the value of their time reasonably incurred to remedy or mitigate the effects of the attack, emotional distress, and the present and certainly imminent risk of future harm caused by the compromise of their Sensitive Information.

6. As part of its services, KeyBank requires that its customers, including Plaintiffs and Class Members, to provide KeyBank with their PII, including, but not limited to names, Social Security numbers, mortgage addresses, telephone numbers, and state identification cards (e.g., Driver's Licenses, State ID Cards, or Passports).

7. As a sophisticated institutions that collected, stored, and maintained the PII of Plaintiffs and Class Members, Defendants owed Plaintiffs and Class Members

numerous statutory, regulatory, contractual, and common law duties and obligations, including those based on its affirmative representations to keep Plaintiffs' and Class Members' PII confidential, safe, secure, and protected from unauthorized disclosure, access, dissemination, or theft.

8. Indeed, during the course if its business operations, Defendants expressly and impliedly promised to safeguard Plaintiffs' and Class Members' PII.

9. Furthermore, by obtaining, collecting, using, retaining, and deriving benefit from Plaintiffs' and Class Members' PII, Defendants assumed legal and equitable duties to Plaintiffs and Class Members and knew or should have known that they were responsible for safeguarding and protecting Plaintiffs' and Class Members' PII from unauthorized disclosure access, dissemination, or theft.

10. Plaintiffs and Class Members provided their PII to KeyBank with the reasonable expectation of privacy and mutual understanding that KeyBank would comply with its legal duties, obligations, and representations to keep such information confidential, safe, and secure.

11. Plaintiffs and Class Members reasonably expected and relied upon KeyBank to not entrust their PII with third party vendors, like OSC, who maintained inadequate data security and retention systems.

12. Plaintiffs and Class Members further reasonably expected and relied upon Defendants to only use their PII for business purposes, implement reasonable

retention and data destruction policies, and to make only authorized disclosures of this information.

13. Plaintiffs and Class Members would not have paid the amounts of money they paid for KeyBank's services, or surrendered their PII, had they known their information would be entrusted to and maintained by OSC, who employed inadequate data security and retention systems.

14. Defendants' data security obligations were particularly important given the substantial increase in data breaches preceding the date of the Data Breach.

15. Defendants breached its duties, promises, and obligations, and Defendants' failures to honor its obligations increased the risk that Plaintiffs' and Class Members' PII would be compromised in the event of a likely cyberattack.

16. Beginning on or about August 26, 2022, KeyBank notified state Attorneys General and/or many of its loan customers about a widespread data breach involving the sensitive PII of thousands of individual loan customers ("Notice Letter").[2] KeyBank explained through its Notice Letter that an unauthorized third party remotely accessed OSC's network and on July 5, 2022, *acquired* certain personal information of KeyBank's clients. KeyBank entrusted its customers PII to a third-party vendor with inadequate data security and retention systems which

[2] Office of the Massachusetts Attorney General, Data Breach Notification, *available at* https://www.mass.gov/doc/assigned-data-beach-number-28146-keybank/download (last visited September 13, 2022).

allowed its network to be accessed by unknown third parties, exposing and allowing access to, and acquisition of, the PII for individual customers detailed above.[3] As an example, KeyBank notified the Texas Attorney General on or around August 30, 2022, that there were 2,186 Texas residents affected by the breach.[4]

17. Presaging the harm that Defendants knew would befall victims of the Data Breach, the Notice Letter also advised Plaintiffs and Class Members "to remain vigilant by closely monitoring your account statements over the next 12 to 24 months." Moreover, recognizing that each Class Member is now subject to the present and continuing risk of identity theft and fraud, Defendants offered Plaintiffs and Class Members credit and identity theft monitoring services for 24 months through Equifax.

18. Notably, even though the Data Breach occurred on July 5, 2022, OSC did not notify KeyBank until August 4, 2022. Compounding the risk to Plaintiffs and Class Members, KeyBank then failed to promptly notify the impacted individuals, waiting three weeks to finally send the data breach notifications to its customers, an unreasonable amount of time from any objective measure.

19. At this phase of litigation, the full extent of the types of sensitive personal information, the scope of the breach, and the root cause of the Data Breach

---

3 *Id.*

4 https://oagtx.force.com/datasecuritybreachreport/apex/DataSecurityReportsPage (last visited September 15, 2022).

are all within the exclusive control of Defendants and its agents, counsel, and forensic security vendors.

20. Upon information and belief, Defendants are responsible for allowing this Data Breach because of multiple acts of negligence, including but not limited to: its failure to design, implement, and maintain reasonable data security systems and safeguards; and/or failure to exercise reasonable care in the hiring, supervision, training, and monitoring of its employees and agents and vendors; and/or failure to comply with industry-standard data security practices; and/or failure to comply with federal and state laws and regulations that govern data security and privacy practices and are intended to protect the type of Sensitive Information at issue in this action; and/or failure to design, implement and execute reasonable data retention and destruction policies.

21. In this era of frequent data security attacks and data breaches, particularly in the financial industry, Defendants' failures leading to the Data Breach are particularly egregious, as this Data Breach was highly foreseeable.

22. Until notified of the breach, Plaintiffs and Class Members were not aware that their PII had been compromised in the Data Breach and that they were, and continue to be, at significant risk of identity theft and various of forms of personal, social, and financial harm. This risk will remain for the rest of their lives.

23. As KeyBank instructed, advised, and warned in its Notice Letters,

Plaintiffs and the Class Members must now closely monitor their financial accounts to guard against future identity theft and fraud. Plaintiffs' and Class Members' have heeded such warnings to mitigate against the imminent risk of future identity theft and financial loss. Such mitigation efforts included and will include into the future: reviewing financial statements, changing passwords, and signing up for credit and identity theft monitoring services. The loss of time and other mitigation costs are tied directly to guarding against and mitigating against the imminent risk of identity theft.

24. Plaintiffs and Class Members have suffered actual and present injuries as a direct result of the Data Breach, including: (a) theft of their PII; (b) costs associated with the detection and prevention of identity theft for their respective lifetimes; (c) costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the consequences of the Data Breach; (d) invasion of privacy; (e) the emotional distress, stress, nuisance, and annoyance of responding to, and resulting from, the Data Breach; (f) the present and/or imminent injury arising from actual and/or potential fraud and identity theft posed by their personal data being placed in the hands of the ill-intentioned hackers and/or criminals; (g) damages to and diminution in value of their personal data entrusted to Defendants on the mutual understanding that Defendants would safeguard their PII against theft and not allow access to and misuse of their personal data by others; and (h) the continued risk to their PII, which remains in the possession of Defendants, and which is subject to further injurious breaches, so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' PII. Plaintiffs and Class Members, at the very least, are entitled to damages and injunctive relief tailored to address the vulnerabilities exploited in the breach, and designed to protect Plaintiffs' and Class Members' PII, as well as an order from the Court directing the destruction and deletion of all PII for which Defendants cannot demonstrate a reasonable and

legitimate purpose for continuing to maintain possession of such PII.

25. Defendants understand the need to protect the privacy of their customers and use security measures to protect their customers' information from unauthorized disclosure.[5] And as sophisticated financial entities who maintain private and sensitive consumer information, Defendants further understood the importance of safeguarding PII. Yet Defendants disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that Plaintiffs and Class members' PII was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As a result, the PII of Plaintiffs and Class Members was compromised through access to and exfiltration by an unknown and unauthorized third party. Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains safe, and they are entitled to injunctive and other equitable relief.

26. Plaintiffs seek to remedy these harms, and to prevent the future

[5] See https://www.oscis.com/privacy/ (last visited September 15, 2022) and See https://www.key.com/about/security/privacy.html ((last visited September 15, 2022).

occurrence of an additional data breach, on behalf of themselves and all similarly situated persons whose PII was compromised as a result of the Data Breach. Plaintiffs seek remedies including, but not limited to, compensatory damages, reimbursement for loss of time, reimbursement of opportunity costs, out-of-pocket costs, price premium damages, and injunctive relief including improvements to Defendant's data security systems and protocols, future annual audits, and adequate credit monitoring services funded by the Defendant.

PARTIES

Plaintiff Mariann Archer

27. Plaintiff Mariann Archer is a citizen of the state of New York and resides in Clinton, New York. Plaintiff Archer is a consumer and former customer of KeyBank. Plaintiff Archer provided her personal information and PII to KeyBank. KeyBank notified Plaintiff Archer of the Data Breach and the unauthorized access of her PII by sending her a Notice of Data Breach letter, dated August 26, 2022.

28. Plaintiff Patrick Reddy is a citizen of the state of Washington and resides in Seattle, Washington. Plaintiff Reddy is a consumer who is a customer of KeyBank and provided personal information and PII to KeyBank. KeyBank notified Mr. Reddy of the Data Breach and the unauthorized access of his PII by sending him a Notice of Data Breach letter, dated August 26, 2022.

29. Defendant KeyBank, N.A. is a National Association under the laws of

the United States and maintains its principal place of business at 127 Public Square, Cleveland, Ohio 44114.

30. Defendant Overby-Seawell Co. is Georgia corporation and maintains its principal place of business at 245 TownPark Drive, Suite 200, Kennesaw, Georgia 30144.

31. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiffs. Plaintiffs will seek leave of court to amend this complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

32. All of Plaintiffs' claims stated herein are asserted against KeyBank, NA and Overby-Seawell Co. and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

JURISDICTION AND VENUE

33. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, and there are more than 100 members in the proposed class. The minimal diversity requirement is met as Plaintiffs, Class Members, and Defendants are citizens of different states.

34. OSC is a citizen of Georgia because it is a Georgia corporation and its principal place of business is in Kennesaw, Georgia. Thus, the Northern District of Georgia has general jurisdiction over OSC.

35. The Northern District of Georgia has personal jurisdiction over OSC because it conducts substantial business in Georgia and this District.

36. The Northern District of Georgia has personal jurisdiction over KeyBank because it shared Plaintiffs' and Class Members' PII with OSC in Georgia and this District.

37. Venue is proper in this District under 28 U.S.C. §1391(b) because OSC operates in this District, KeyBank provided and entrusted Plaintiffs' and Class Members' PII to OSC in this District, and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District.

BACKGROUND

38. KeyBank is "one of the nation's largest bank-based financial services companies, with assets of approximately $186 billion."[6] KeyBank operates community banking centers in 15 states and corporate banking offices throughout the United States KeyBank and has annual revenues of $1.7 billion.[7] As of December 31, 2021, KeyBank had 999 full-service branch locations, including

[6] *Id.*

[7] https://www.key.com/about/company-information/key-company-overview.html (last visited September 6, 2022)

branch locations in the states of New York and Washington, and employed 17,654 full employees.[8]

39. KeyBank is a full-service mortgage lender, offering fixed- and adjustable-rate conventional mortgages, specialty mortgages including combination or piggyback loans and jumbo loans, and affordable mortgages like Key Community, FHA, Fannie Mae and VA loans, as well as mortgages specifically for medical professionals.

40. KeyBank has acknowledged the sensitive and confidential nature of the PII it collects from its customers.

41. Collecting, maintaining, retaining, and protecting PII is vital to many of KeyBank's business purposes.[9] Furthermore, KeyBank has acknowledged through conduct and statements that the PII should only be used for a legitimate business purpose, that the misuse or inadvertent access, disclosure or unauthorized dissemination of PII can pose major privacy and financial risks to impacted individuals, and that they may not disclose and must take reasonable steps to protect PII from improper release or disclosure.[10]

42. With respect to privacy in general, KeyBank knows that its customers

---

[8] KeyCorp (2021). Form 10-K https://www.sec.gov/Archives/edgar/data/91576/000009157622000029/key-20211231.htm
[9] See *Id.*
[10] See *Id*.

"value your privacy… That's why KeyBank is dedicated to safeguarding your banking information…. Using the latest technology and sophisticated tools, we work to keep your personal and business data protected."[11]

43. As a sophisticated financing institution, KeyBank knew, or should have known, that Plaintiffs' and Class Members' PII, that KeyBank collected and maintained, was a target of data thieves and that it had a duty to protect Plaintiffs' and Class Members' PII from unauthorized access. On its website KeyBank states that, "Your security and privacy are our highest priority" and that it "treats your information with care."[12]

44. KeyBank relies on third-party vendors, like OSC, to perform "significant operational services" for it.[13]

45. OSC is a third-party vendor for KeyBank that provides ongoing verification that KeyBank's residential mortgage clients are maintaining property insurance on their real estate.

46. OSC describes itself as "a leading provider of compliance-driven tracking technology and insurance products and services for lenders, mortgage servicers, finance companies, and property investors." [14]

---

[11] https://www.key.com/about/security/privacy.html (last visited September 6, 2022).
[12] https://www.key.com/about/security/consumer-security.html (last visited September 6, 2022).
[13] KeyCorp (2021). Form 10-K https://www.sec.gov/Archives/edgar/data/91576/00000915762 2000029/key-20211231.htm (last visited September 14, 2022)
[14]https://www.oscis.com/wp-content/uploads/2018/04/OSC-Overview-011922.pdf (last visited September 14, 2022).

47. OSC boasts that "at the core all we do is a strict adherence to compliance best practices, rigorous security on and off-line, quality-control measures, and multifaceted corporate governance checks and balances."[15]

48. OSC was also aware of the sensitive nature of the PII that KeyBank entrusted it with. On its website, OSC's privacy physical policy outlines that it has "electronic, and procedural safeguards in order to protect any nonpublic personal information we maintain regarding our Participants."[16]

49. Plaintiffs and Class Members, relied on these express and implied promises and on these sophisticated Defendants to keep their sensitive PII confidential and securely maintained, to use this information for business purposes only, to implement reasonable retention policies, to limit access to authorized individuals, and to make only authorized disclosures of this information.

50. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' PII, Defendants assumed legal and equitable duties to these individuals to safeguard and protect the PII from unauthorized access.

THE DATA BREACH AND DEFENDANTS' RESPONSE

51. On or around July 5, 2022, an intruder gained unauthorized access to

[15] *Id.*
[16] *Id.*

OSC's network.[17] Before being discovered, the intruder accessed and acquired the PII of thousands of KeyBank's customers.[18]

52. On or around August 4, 2022, OSC notified Key Bank that KeyBank's clients' and customer' PII was compromised in the Data Breach.

53. Beginning on or about August 26, 2022, KeyBank reported the Data Breach to the various attorneys general offices, including those in California, Maine, Massachusetts, Texas, among other states. On that same date, it also began notifying Plaintiffs and Class Members of the Data Breach.

54. The PII that was accessed without authorization included names, along with data elements including the first eight digits of Social Security numbers, mortgage property addresses, mortgage account numbers, mortgage account information, telephone numbers, property information, and home insurance policy numbers and information.

55. Upon information and belief, the PII was not encrypted or was not adequately encrypted prior to the Data Breach.

56. Thus, for approximately one month, unauthorized third parties had access to KeyBank's trove of highly sensitive and PII before OSC even notified

[17] Office of the California Attorney General, Data Breach Notification, *available at* https://oag.ca.gov/system/files/Notice%20of%20Data%20Breach%20%28CA%29.pdf. (last visited September 13, 2022).
[18] Office of the Attorney General of Texas, Data Security Breaches, *available* at https://oagtx.force.com/datasecuritybreachreport/apex/DataSecurityReportsPage; (initially reporting 2186 Texans impacted) (last visited September 13, 2022).

KeyBank of the Data Breach.

57. Even though Key Bank received notice from OSC on August 4, 2022, that KeyBank's clients' PII was compromised in the Data Breach, KeyBank still took nearly three weeks to notify state Attorneys General and Class Members about the Data Breach. Even then, KeyBank did not fully disclose the scope of the Data Breach but opted to issue a vague letter leaving Plaintiffs and Class Members without a full understanding of how the breach occurred or what happened to their PII once it was accessed.

DEFENDANTS ACQUIRE, COLLECT, AND STORE PLAINTIFFS' AND CLASS MEMBERS' PII

58. Defendants acquired, collected, and stored the PII of Plaintiffs and Class Members.

59. In the course and scope of its residential mortgage financing business, KeyBank collects massive amounts of highly sensitive PII, including but not limited to, Social Security numbers, employment information (including tax returns, W-2's, pay stubs, and letters regarding employment history), assets, credit histories and letters regarding credit events, investment information, addresses, dates of birth, and driver's license information.[19]

60. By obtaining, collecting, and storing Plaintiffs' and Class Members'

[19] https://www.key.com/personal/financial-wellness/articles/prequal-checklist-for-a-home-loan.html (last visited September 6, 2022).

PII, Defendants assumed legal and equitable duties and knew or should have known that they were responsible for protecting Plaintiffs' and Class Members' PII from disclosure.

61. Collecting, maintaining, and protecting PII is vital to many of KeyBank's business purposes. In its 2021 Annual Report, KeyBank notes, "a significant portion of our operations relies heavily on the secure processing, storage, and transmission of personal and confidential information, such as the personal information of our customers and clients."[20]

62. Plaintiffs and Class Members entrusted their PII to KeyBank on the premise and with the understanding that KeyBank would safeguard their information, use their PII for business purposes only, and/or not disclose their KeyBank to unauthorized third parties, and/or not share PII with third-party vendors with inadequate data security systems, and/or only retain PII for necessary business purposes and for a reasonable amount of time.

PLAINTIFFS AND CLASS MEMBERS WERE INJURED BY DEFENDANTS' FAILURE TO SECURE THEIR SENSITVE INFORMATION

[20] KeyCorp (2021). Form 10-K. https://sec.report/Document/0000091576-21-000044/

63. Defendants could have prevented this Data Breach by properly securing and encrypting Plaintiffs' and Class Members' PII. Additionally, Defendants could have destroyed data, including old data that Defendants had no legal right or responsibility to retain.

64. Defendants knew that the PII they maintained was a target of data thieves and that they had a duty to protect Plaintiffs' and Class Members' PII from unauthorized access.

65. In its notice letter, KeyBank issued an express warning and advised Plaintiffs and Class Members of the seriousness of the attack, and that they should "remain vigilant" and immediately sign up for identity theft protection. The Notice Letter further issued specific instructions and mitigation techniques such as "closely monitoring your account statements over the next 12 to 24 months"– KeyBank instructed customers to:

- Remain vigilant by closely monitoring your account statements over the next 12 to 24 months;

- Promptly report any suspicious account activity related to you KeyBank account(s) by calling the Fraud and Disputes Hotline at 1-800-433-0124. Promptly report any fraudulent activity or suspected identity theft to the law enforcement authorities of other financial institutions as applicable;

- Enroll in Equifax Complete Premier online credit monitoring service.

66. These warnings and instructions are an acknowledgment by KeyBank

that it is not only plausible that the criminals acquired the PII for criminal purposes, thereby placing the impacted customers at an imminent threat of identity theft and financial fraud – but that the theft and dissemination and misuse of the PII is the highly probable result of this type of cyberattack and a present threat to all Class Members.

67. Without the likelihood of dissemination and misuse, and materialization of identity theft, the warnings and instructions to mitigate the risk would be unnecessary and would cause more harm than good, and Defendant would not have advised such actions that would cost Plaintiffs and Class Members time and money.

68. As an additional line of protection, OSC paid for a program that offered identity theft protection services to Class Members. Absent an actual, materialized, and imminent threat to the Plaintiffs and Class Members, such a program would also have been unnecessary and a waste of Defendant's time and money. OSC would not have spent resources offering such a program without the likelihood that the Class Member PII was exfiltrated and disseminated in the attack, and that a materialized and imminent risk of identity theft was present for all Class Members. KeyBank acknowledged the imminent risks to Class Members by encouraging Class Members to enroll in the identity theft protection program:

> **We encourage you to take advantage of a complimentary two-year membership to Equifax® Complete™ Premier made possible by**

> **OSC.** This service helps detect possible misuse of your pe you with identity protection support focused on identification and resolution of identity theft…We strongly encourage you to take advantage of the complimentary Equifax membership as an extra security measure.[21]

69. Finally, KeyBank also acknowledged the OSC purported to "deploy enhanced security monitoring tools across their network and notified the Federal Bureau of Investigation (FBI) of this incident."

70. While KeyBank admits enhanced "security monitoring tools" were required to improve its OSC's data security systems, there is no indication based solely on the Notice Letter whether these steps are fully adequate to protect Plaintiffs' and Class Members' PII going forward, as the source and root cause of the data breach were not disclosed and remain unknown and undiscoverable absent litigation.[22]

71. What is evident and indisputable is that the Data Breach resulted in the unauthorized access of OSC's systems and files, and that those compromised files contained the PII of Plaintiffs and thousands of Class Members including their names, first eight digits of their Social Security numbers, mortgage property address, mortgage account numbers, mortgage account information, phone numbers, property information, and home insurance policy numbers and information.

72. Upon information and belief, the cyberattack targeted OSC due to

---

[21] August 26, 2022, letter to the Attorney General of California, supra n.2.
[22] *Id.*

OSC's status as a vendor for KeyBank, a national, multi-billion-dollar bank, that routinely collects valuable personal and financial data on its many customers, including Plaintiffs and Class Members.

73. Upon information and belief, the cyberattack was expressly designed to gain access to and steal the private and confidential data, including (among other things) the PII of Plaintiffs and the Class Members.

74. As a result of the Data Breach, the risk of identity theft has materialized, and Plaintiffs and Class Members are at an imminent risk of identity theft and other financial crimes.

THE DATA BREACH WAS FORESEEABLE

75. Defendants' data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the financial industry and other industries holding significant amounts of PII preceding the date of the breach.

76. In light of recent high profile data breaches at other industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), KeyBank knew or should have known that its systems would be targeted by cybercriminals.

77. Indeed, cyberattacks against the financial industry have been common for over ten years with the FBI warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII." The FBI further warned that that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime."[23]

78. In its 2021 Annual Statement, KeyBank acknowledges that cyber-attacks are an operational risk and that, "other U.S. financial service institutions and companies have reported breaches, some severe, in the security of their websites or other systems and several financial institutions, *including Key*, have experienced significant distributed denial-of-service attacks, some of which involved sophisticated and targeted attacks intended to disable or degrade service, or sabotage systems."[24]

79. As a sophisticated financial and insurance institutions that collect, utilize, and store particularly sensitive PII, Defendants were at all times fully aware of the increasing risks of cyber-attacks targeting the PII it controlled, and its obligation to protect the PII of Plaintiffs and Class Members.

---

23 Gordon M. Snow, Statement before the House Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit, FBI (Sept. 14, 2011), https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector.

[24] KeyCorp (2021). Form 10-K. https://sec.report/Document/0000091576-21-000044/

80. Importantly, KeyBank was particularly aware that it exposed its customers to additional cyber security risks by entrusting Plaintiffs' and Class Members' PII to Defendant OSC. "We are also exposed to operational risk through our outsourcing arrangements…"[25]

81. KeyBank admits that the use of third-party vendors, like Defendant OSC, increases the risks to their customers of a data security breach. KeyBank notes, "In the event of a failure, interruption, or breach of our information systems or that of a third party that provides services to us or our customers, we may be unable to avoid impact to our customers."[26]

82. Plaintiffs and Class Members now currently face years of constant surveillance and monitoring of their financial and personal records and loss of rights. Plaintiffs and Class Members are incurring, and will continue to incur, such damages in addition to any fraudulent use of their PII.

83. The injuries to Plaintiffs and Class Members are directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the PII of Plaintiffs and Class Members, and such as encrypting the data so unauthorized third parties could not see the PII.

DEFENDANTS FAILED TO PROTECT PLAINTIFFS' AND CLASS MEMBERS' PII

---

[25] *Id.*
[26] *Id.*

84. Despite the prevalence of public announcements of data breach and data security compromises, and despite Defendant's own acknowledgment of its duties to keep PII private and secure, Defendants failed to take appropriate steps to protect the PII of Plaintiffs and the Class from being compromised.

85. KeyBank was aware that it could not properly maintain or manage the Sensitive Information entrusted to it by Plaintiffs and Class Members, nor could it sufficiently compensate or protect its clients when that Sensitive Information is compromised by third-party vendors OSC.

86. Regarding the risks associated with using third-party vendors like OSC, KeyBank notes, "To the extent that we use third parties to provide services to our clients, we seek to minimize the risk by performing due diligence and monitoring the third party, but we cannot control all of the risks at these third parties…. Should an adverse event affecting another company's systems occur, we may not have indemnification or other protection from the other company sufficient to fully compensate us or otherwise protect us or our clients from the consequences."[27]

87. KeyBank negligently entrusted duties to safeguard Plaintiffs' and Class Members' PII to OSC without performing due diligence or adequately monitoring, inspecting, or controlling OSC's data security practices.

88. KeyBank negligently supervised OSC and failed to require OSC to

[27] *Id.*

implement, maintain, and to sufficiently upgrade OSC's data security systems and protocols.

89. Defendants did not use reasonable security procedures and practices appropriate to the nature of the Sensitive Information it was maintaining for Plaintiffs and Class Members, causing the exposure of Plaintiffs and Class Members' PII.

A. Defendants Failed to Properly Comply with Federal Trade Commission Data Security Standards

90. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making.

91. The FTC has brought well publicized enforcement actions against businesses for failing to adequately and reasonably protect consumer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. This includes the FTC's enforcement action against Equifax following a massive data breach involving the personal and financial information of 147 million Americans.

92. In 2016, the FTC updated its publication, "Protecting Personal

Information: A Guide for Business," which established cyber-security guidelines for businesses that Defendants did not adequately employ. The FTC advised that businesses like Defendants should protect the PII that they keep by following some minimum standards related to data security, including, among others:

(a) Encrypting information stored on computer networks;

(b) Identifying network vulnerabilities;

(c) Implementing policies to update and correct any security problems;

(d) Utilizing an intrusion detection systems;

(e) Monitor all incoming traffic for suspicious activity indicating someone is attempting to hack the system;

(f) Watching for large amounts of data being transmitted from the system;

(g) Developing a response plan ready in the event of a breach;

(h) Limiting employee and vendor access to sensitive data;

(i) Requiting complex passwords to be used on networks;

(j) Utilizing industry-tested methods for security;

(k) Verifying that third-party service providers have implemented reasonable security measures;

(l) Educating and training employees on data security practices;

(m) Implementing multi-layer security including firewalls, anti-virus, and anti-malware software;

(n) Implementing multi-factor authentication.

93. In particular, the FTC further advised that companies not maintain PII

longer than is needed for authorization of a transaction: "If you don't have a legitimate business need for sensitive personally identifying information, don't keep it."[28]

94. Upon information and belief, Defendants failed to implement or adequately implement at least one of these fundamental data security practices.

95. Defendants could have prevented this Data Breach by properly following FTC guidelines by adequately encrypting or otherwise protecting their equipment and computer files containing PII.

96. Defendants to employ reasonable and appropriate measures to protect against unauthorized access to customers' PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

B. Defendants Failed to Comply with Industry Standards

97. The financial industry also routinely incorporates these cybersecurity practices that are standard in the financial industry, and that Defendants did not adequately employ. These minimum standards include but are not limited to:

(o) Maintaining a secure firewall configuration;

(p) Maintaining appropriate design, systems, and controls to limit user access to certain information as necessary;

(q) Monitoring for suspicious or irregular traffic to servers;

[28] FTC, Protecting Personal Information: A Guide for Business (Oct. 2016), https://www/ftc.gov/business-guidance/resources/protecting-personal-information-guide-business.

(r) Monitoring for suspicious credentials used to access servers;

(s) Monitoring for suspicious or irregular activity by known users;

(t) Monitoring for suspicious or unknown users;

(u) Monitoring for suspicious or irregular server requests;

(v) Monitoring for server requests for PII;

(w) Monitoring for server requests from VPNs; and

(x) Monitoring for server requests from Tor exit nodes.

98. Upon information and belief, Defendants failed to comply with at least one of these minimal industry standards, thereby opening the door to, and causing the Data Breach.

99. Defendants could have prevented this Data Breach by properly following industry data security standards by adequately encrypting or otherwise protecting their equipment and computer files containing PII.

100. Defendants could also have prevented the scale of the Data Breach simply by designing and implementing data retention practices to delete PII that is no longer needed for an ongoing business purpose.

101. Defendants had the resources necessary, and reasonable data security alternatives were known and available to Defendants that would have prevented the Data Breach, but Defendants neglected to adequately evaluate its systems, and invest in adequate security measures, despite its obligation to protect its systems and Plaintiffs' and Class Members' PII.

C. KeyBank Failed to Comply with Gramm-Leach-Bliley Act

102. KeyBank is a financial institution, as that term is defined by Section 509(3)(A) of the Gramm-Leach-Bliley Act ("GLBA"), 15 U.S.C. § 6809(3)(A), and thus is subject to the GLBA.

103. The GLBA defines a financial institution as "any institution the business of which is engaging in financial activities as described in Section 1843(k) of Title 12 [the Bank Holding Company Act of 1956]." 15 U.S.C. § 6809(3)(A).

104. KeyBank collects nonpublic personal information, as defined by 15 U.S.C. § 6809(4)(A), 16 C.F.R. § 313.3(n) and 12 C.F.R. § 1016.3(p)(1). Accordingly, during the relevant time period Defendant was subject to the requirements of the GLBA, 15 U.S.C. § 6801.1, *et seq.*, and is subject to numerous rules and regulations promulgated on the GLBA Statutes. The GLBA Privacy Rule became effective on July 1, 2001. *See* 16 C.F.R. § 313. Since the enactment of the Dodd-Frank Act on July 21, 2010, the CFPB became responsible for implementing the Privacy Rule. In December 2011, the CFPB restated the implementing regulations in an interim final rule that established the Privacy of Consumer Financial Information, Regulation P, 12 C.F.R. § 1016 ("Regulation P"), with the final version becoming effective on October 28, 2014.

105. Accordingly, KeyBank's conduct is governed by the Privacy Rule prior to December 30, 2011, and by Regulation P after that date.

106. Both the Privacy Rule and Regulation P require financial institutions to provide customers with an initial and annual privacy notice. These privacy notices must be "clear and conspicuous." 16 C.F.R. §§ 313.4(a) and 313.5(a)(1); 12 C.F.R. §§ 1016.4 and 1016.5. "Clear and conspicuous means that a notice is reasonably understandable and designed to call attention to the nature and significance of the information in the notice." 16 C.F.R. § 313.3(b)(1); 12 C.F.R. § 1016.3(b)(1). These privacy notices must "accurately reflect[] [the financial institution's] privacy policies and practices." 16 C.F.R. § 313.4(a)(1) and 313.5(a)(1); 12 C.F.R. §§ 1016.4 and 1016.5. They must include specified elements, including the categories of nonpublic personal information the financial institution collects and discloses, the categories of third parties to whom the financial institution discloses the information, and the financial institution's security and confidentiality policies and practices for nonpublic personal information. 16 C.F.R. § 313.6; 12 C.F.R. § 1016.6. These privacy notices must be provided "so that each consumer can reasonably be expected to receive actual notice." 16 C.F.R. § 313.9(a); 12 C.F.R. § 1016.9. As alleged herein, KeyBank violated the Privacy Rule and Regulation P.

107. Upon information and belief, KeyBank failed to provide annual privacy notices to customers after the customer relationship ended, despite retaining these customers' PII and storing and/or sharing that PII on its network.

108. KeyBank failed to adequately inform its customers that it was storing

and/or sharing, or would store and/or share, the customers' PII on its inadequately secured network and would do so after the customer relationship ended.

109. The Safeguards Rule, which implements Section 501(b) of the GLBA, 15 U.S.C. § 6801(b), requires financial institutions to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards, including: (a) designating one or more employees to coordinate the information security program; (b) identifying reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information, and assessing the sufficiency of any safeguards in place to control those risks; (c) designing and implementing information safeguards to control the risks identified through risk assessment, and regularly testing or otherwise monitoring the effectiveness of the safeguards' key controls, systems, and procedures; (d) overseeing service providers and requiring them by contract to protect the security and confidentiality of customer information; and (e) evaluating and adjusting the information security program In light of the results of testing and monitoring, changes to the business operation, and other relevant circumstances. 16 C.F.R. §§ 314.3 and 314.4. As alleged herein, Defendant violated the Safeguard Rule.

110. KeyBank failed to assess reasonably foreseeable risks to its and OSC's

networks, and the security, confidentiality, and integrity of PII in its custody or control.

111. KeyBank failed to design and implement information safeguards to control the risks identified through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.

112. KeyBank failed to adequately oversee service providers, including OSC.

113. KeyBank failed to evaluate and adjust its information security program in light of the results of testing and monitoring, changes to the business operation, and other relevant circumstances.

THE VALUE OF PII

114. There is both a healthy black market and a legitimate market for the type of PII that was compromised in this action. PII is such a valuable commodity to criminal networks that once the information has been compromised, criminals often trade the information on the "cyber black market" for years.

115. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the Dark Web. Numerous sources cite Dark Web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to

$200.[29]

116. According to the Dark Web Price Index for 2021, payment card details for an account balance up to $1,000 have an average market value of $150, credit card details with an account balance up to $5,000 have an average market value of $240, stolen online banking logins with a minimum of $100 on the account have an average market value of $40, and stolen online banking logins with a minimum of $2,000 on the account have an average market value of $120.[30] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[31]

117. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, when they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought.

---

[29] Anita George, Your personal data is for sale on the dark web. Here's how much it costs, Digital Trends (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/.

[30] Zachary Ignoffo, Dark Web Price Index 2021, Privacy Affairs (Mar. 8, 2021), https://www.privacyaffairs.com/dark-web-price-index-2021/.

[31] In the Dark, VPNOverview (2019), https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/.

> Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[32]

118. The Social Security Administration has further warned that identity thieves can use an individual's Social Security number to apply for additional credit lines. Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, apply for a job using a false identity, open bank accounts, and apply for other government documents such as driver's license and birth certificates.

119. Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are not typically discovered until an individual's authentic tax return is rejected.

120. What's more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to

---

[32] Social Security Administration, Identity Theft and Your Social Security Number (June 2021), https://www.ssa.gov/pubs/EN-05-10064.pdf.

obtain a new number.

121. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[33]

122. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x in price on the black market."[34]

PLAINTIFFS AND CLASS MEMBERS SUFFERED FORESEEABLE CONCRETE HARMS

123. As a result of Defendants ineffective and inadequate data security and retention measures, the Data Breach, and the foreseeable consequences of the PII ending up in the possession of criminals, the risk of identity theft is materialized and imminent.

124. Given the type of targeted attack in this case and sophisticated criminal

---

[33] Brian Naylor, Victims Of Social Security Number Theft Find It's Hard To Bounce Back, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft.

[34] Tim Greene, Anthem hack: Personal data stolen sells for 10x price of stolen credit card numbers, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

activity, the type of PII there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/Dark Web for sale and purchase by criminals intending to utilize the PII for identity theft crimes, such as opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; or file false unemployment claims.

125. Furthermore, the information accessed and disseminated in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, where victims can easily cancel or close credit and debit card accounts.[35] The information disclosed in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers).

126. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. The fraudulent activity resulting from the Data Breach may not become evident for years.

127. Indeed, "[t]he risk level is growing for anyone whose information is stolen in a data breach."[36] Javelin Strategy & Research, a leading provider of quantitative and qualitative research, notes that "[t]he theft of SSNs places

---

[35] See Jesse Damiani, Your Social Security Number Costs $4 On The Dark Web, New Report Finds, Forbes (Mar. 25, 2020), https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1.

[36] Susan Ladika, Study: Data Breaches Pose a Greater Risk, Fox Business (Mar. 6, 2016), https://www.foxbusiness.com/features/study-data-breaches-pose-a-greater-risk.

consumers at a substantial risk of fraud."[37] Moreover, there is a high likelihood that significant identity fraud and/or identity theft has not yet been discovered or reported. Even data that have not yet been exploited by cybercriminals bears a high risk that the cybercriminals who now possess Class Members' PII will do so at a later date or re-sell it.

128. To date, Defendants have done little to adequately protect Plaintiffs and Class Members, or to compensate them for their injuries sustained in this data breach. The complimentary fraud and identity monitoring service offered by OSC is wholly inadequate as the service is only offered for 24 months and it places the burden squarely on Plaintiffs and Class Members by requiring them to expend time signing up for that service, as opposed to automatically enrolling all victims of this cybercrime.

129. Thus, due to the actual and imminent risk of identity theft, Plaintiffs and Class Members must, in KeyBank's words, "remain vigilant" and monitor their financial accounts for many years to mitigate the risk of identity theft.

130. Plaintiffs and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as placing "freezes" and "alerts" with credit reporting agencies, contacting financial institutions, closing or

---

[37] The Consumer Data Insecurity Report: Examining The Data Breach- Identity Fraud Paradigm In Four Major Metropolitan Areas, Al Pascal, 2014), https://www.it.northwestern.edu/bin/docs/TheConsumerDataInsecurityReport_byNCL.pdf.

modifying financial accounts, changing passwords, reviewing and monitoring credit reports and accounts for unauthorized activity, and filing police reports, which may take years to discover and detect.

131. Plaintiffs' mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[38]

132. Plaintiffs' mitigation efforts are also consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[39]

133. Furthermore, Defendants poor data security deprived Plaintiffs and Class Members of the benefit of their bargain. When agreeing to pay KeyBank and/or its affiliated vendors for services, Plaintiffs and Class Members understood

[38] See United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), https://www.gao.gov/new.items/d07737.pdf.

[39] See Federal Trade Commission, Identity Theft.gov, https://www.identitytheft.gov/Steps (last visited July 7, 2022).

and expected that they were paying for services and data security, when in fact, Defendants did not provide the expected data security. Accordingly, Plaintiffs and Class Members received services that were of a lesser value than what they reasonably expected.

134. As a result of Defendants' ineffective and inadequate data security and retention measures, the Data Breach, and the imminent risk of identity theft, Plaintiffs and Class Members have suffered numerous actual and concrete injuries, including: (a) invasion of privacy; (b) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) financial "out of pocket" costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g) the loss of benefit of the bargain (price premium damages); (h) deprivation of value of their PII; and (i) the continued risk to their PII, which remains in the possession of Defendants, and which is subject to further breaches, so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' Sensitive Information.

PLAINTIFFS' COMMON EXPERIENCES

Plaintiff Mariann Archer's Experience

135. Prior to the Data Breach, KeyBank serviced Plaintiff Archer's mortgage loan. Plaintiff Archer made monthly mortgage payments to KeyBank.

136. By virtue of servicing Plaintiff Archer's mortgage loan, KeyBank acquired significant personal, income, and financial information of Plaintiff Archer.

137. Plaintiff Archer greatly values her privacy and Sensitive Information, especially when receiving loan and financial services. Plaintiff Archer has taken reasonable steps to maintain the confidentiality of her PII, and she has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

138. Plaintiff Archer stores any and all documents containing PII in a secure location and destroys any documents she receives in the mail that contain any PII or that may contain any information that could otherwise be used to compromise her identity and financial accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts. In addition, she does not release her birthdate or other PII on social media sites, *etc.*, as a precautionary measure from identity fraud.

139. Plaintiff Archer received a Notice Letter from KeyBank, dated August 26, 2022, informing her that her full name, mortgage property address, mortgage account number(s) and mortgage account information, telephone number, property information, the first eight digits of her Social Security number, and her home

insurance policy number and home insurance information were acquired by unauthorized third parties.

140. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Archer faces, Defendant KeyBank encouraged Plaintiff Archer to sign-up for a complimentary two-year membership to credit monitoring services offered by Defendant OSC. This offer is inadequate because data breach victims commonly face many years of ongoing identity theft.

141. As a result of the Data Breach, Plaintiff Archer has suffered a loss of time and has spent, and continues to spend, a considerable amount of time on issues related to the Data Breach.

142. Plaintiff Archer expected and reasonably relied upon Defendants as part of their services to provide adequate data security to protect the PII that she entrusted to KeyBank. If Plaintiff Archer had known that KeyBank would not adequately protect her PII, or that KeyBank would share her PII with OSC, who maintained inadequate and ineffective data security measures, she would not have allowed KeyBank access to this PII and would not have engaged in business with KeyBank.

143. As a result of the Data Breach and the directives that she received in the Notice Letter, Plaintiff Archer has already spent precious hours dealing with the consequences of the Data Breach (*e.g.*, self-monitoring her bank and credit accounts),

as well as her time spent verifying the legitimacy of the Notice of Data Breach, communicating with her bank, and researching multiple forms of security protection services. This time has been lost forever and cannot be recaptured.

144. Moreover, Plaintiff Archer spent this time at Defendant's direction. The Notice Letter Plaintiff Archer received from KeyBank directed Plaintiff Archer to spend time mitigating her losses and to "remain vigilant by closely monitoring your account statements over the next 12 to 24 months."

145. Plaintiff Archer has suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to: (a) damage to and deprivation in the value of her PII, a form of property that Defendant obtained from the Plaintiff; (b) violation of her privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

146. Plaintiff Archer also lost the benefit of the bargain and price premium damages for the services she paid for. Had she known that KeyBank would have inadequate data security practices, or that KeyBank would negligently entrust her PII with OSC, who maintained inadequate and ineffective data security measures, she would not have entered into a business transaction, paid for the services, or provided her PII.

147. Plaintiff Archer has suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns

for the loss of her privacy.

148. Plaintiff Archer has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her stolen PII, especially her first eight digits of her Social Security number, combined with information about her home, being placed in the hands of unauthorized third-party intruders and possibly criminals.

149. Plaintiff Archer has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff Patrick Reddy's Experience

150. Prior to the Data Breach, Plaintiff Reddy provided his PII to KeyBank during the course of a mortgage application. Plaintiff Reddy also paid KeyBank a fee for its services.

151. Plaintiff Reddy greatly values his privacy and Sensitive Information, especially when receiving loan and financial services. Plaintiff Reddy has taken reasonable steps to maintain the confidentiality of his PII, and he has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

152. Plaintiff Reddy is extremely careful about sharing his PII and has never knowingly transmitted unencrypted PII over the internet or any other unsecured

source. He stores any and all documents containing PII in a secure location and destroys any documents he receives in the mail that contain any PII or that may contain any information that could otherwise be used to compromise his identity and financial accounts. Moreover, he diligently chooses unique usernames and passwords for her various online accounts. In addition, he password-protects documents containing PII, and does not release his birthdate or other PII on social media sites, *etc.*, as a precautionary measure from identity fraud.

153. Plaintiff Reddy received a Notice Letter from KeyBank, dated August 26, 2022, informing him that his full name, mortgage property address, mortgage account number(s) and mortgage account information, telephone number, property information, the first eight digits of his Social Security number, and his home insurance policy number and home insurance information were acquired by unauthorized third parties. In the Notice Letter, KeyBank advised him to take certain steps to protect his PII and otherwise mitigate his damages.

154. Plaintiff Reddy expected and reasonably relied upon KeyBank as part of its services to provide adequate data security to protect the PII that he entrusted to KeyBank. If Plaintiff Reddy had known that KeyBank would not adequately protect his PII, he would not have allowed KeyBank access to this PII, and would not have engaged in business with KeyBank.

155. Moreover, as a result of the Data Breach and the directives that he

received in the Notice Letter, Plaintiff Reddy has already spent precious hours dealing with the consequences of the Data Breach (*e.g.*, self-monitoring his bank and credit accounts and reviewing his credit monitoring service), as well as his time spent verifying the legitimacy of the Notice of Data Breach, communicating with his bank, and researching multiple forms of security protection services. This time has been lost forever and cannot be recaptured.

156. Moreover, Plaintiff Reddy spent this time at Defendant's direction. The notice letter Plaintiff Reddy received from KeyBank directed him to spend time mitigating his losses and to "remain vigilant by closely monitoring your account statements over the next 12 to 24 months." To date, he has already spent at least four hours dealing with the consequences of the Data Breach.

157. Plaintiff Reddy retained identity theft and credit monitoring services as a result of the Data Breach, paying $65 per month due to the sensitivity of the stolen PII.

158. Plaintiff Reddy has suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (a) damage to and deprivation in the value of his PII, a form of property that Defendant obtained from the Plaintiff; (b) violation of his privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

159. Plaintiff Reddy also lost the benefit of the bargain and price premium damages for the services he paid. Had he known that KeyBank had inadequate data security practices, he would not have entered into a business transaction, paid for the services, or provided his PII.

160. Plaintiff Reddy has suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach since he received the Notice Letter. Plaintiff Reddy is especially concerned about the theft of his full name paired with the first eight digits of his Social Security number and mortgage account and insurance information.

161. Plaintiff Reddy has suffered present, imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his stolen PII, especially his Social Security number, being placed in the hands of unauthorized third parties and possibly criminals.

162. Plaintiff Reddy has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in KeyBank's possession, is protected and safeguarded from future breaches.

CLASS ALLEGATIONS

163. Plaintiffs Pursuant to Fed. R. Civ. P. 23(a), 23(b)(1), 23(b)(2), 23(b)(3), 23(c)(4) and/or 23(c)(5), Plaintiffs bring this Action on behalf of themselves and on behalf of all other persons similarly situated. Plaintiffs propose the following Class

and Subclass definitions, subject to amendment as appropriate:

The Class

> All individuals residing in the United States whose PII was accessed or exfiltrated during the Data Breach announced by KeyBank in 2022 (the "Nationwide Class"). Under Rule 23, and in the alternative to claims asserted on behalf of the Nationwide Class, Plaintiffs assert claims on behalf of a separate subclass, defined as follows:

The New York Subclass

> All individuals residing in the state of New York whose PII was accessed or exfiltrated during the Data Breach announced by KeyBank in 2022 (the "New York Class").

The Washington Subclass

> All individuals residing in the state of Washington whose PII was accessed or exfiltrated during the Data Breach announced by KeyBank in 2022 (the "Washington Class").

164. The Nationwide Class, New York Subclass, and Washington Subclass are collectively referred herein as the "Class."

165. The Subclasses are collectively referred to herein as the "State Subclasses."

166. Excluded from the Class and the State Subclasses are Defendants, any entity in which either Defendants have a controlling interest, and either Defendants' officers, directors, legal representatives, successors, subsidiaries, and agents; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and any and all federal, state or local

governments, including, but not limited to, their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions. Also excluded from the Class are any judicial officers presiding over this matter, members of their immediate family, and members of their judicial staff.

167. Plaintiffs reserve the right to modify or amend the definitions of the proposed Class and Subclasses before the Court determines whether certification is appropriate.

168. Numerosity, Fed R. Civ. P. 23(a)(1): The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiffs at this time, based on information and belief, the Class consists of thousands of individuals whose sensitive data was compromised in the Data Breach. The alternative New York and Washington Subclasses more than likely contain thousands of Class Members throughout each of the states. The number and identities of Class Members can be ascertained through Defendants' records.

169. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

(a) Whether Defendants breached a duty to Class Members to safeguard their PII;

(b) Whether Defendants expressly or impliedly promised to safeguard the PII of Plaintiffs and Class Members;

(c) Whether Defendants unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' PII;

(d) Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

(e) Whether Defendants' data security systems prior to, during, and after the Data Breach complied with the applicable FTC data security laws and regulations;

(f) Whether Defendants' data security systems prior to and during the Data Breach were consistent with industry standards, as applicable;

(g) Whether unauthorized third parties accessed or obtained Class Members PII in the Data Breach;

(h) Whether Defendants knew or should have known that its data security systems and monitoring processes were deficient;

(i) Whether the Plaintiffs and Class Members suffered legally cognizable injuries as a result of Defendants' misconduct;

(j) Whether Defendants' conduct was negligent;

(k) Whether Defendants breached expressed or implied contractual obligations;

(l) Whether Defendants violated state consumer protections statutes;

(m) Whether Defendants were unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiffs and Class Members;

(n) Whether Defendants failed to provide notice of the Data Breach in a timely manner;

(o) Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

(p) Whether Plaintiffs and Class Members are entitled to damages, restitution, and/or civil penalties; and

(q) Whether Defendants violated state statutes as alleged herein;

170. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' PII, like that of every other Class Member, was compromised in the Data Breach due to Defendants' misfeasance, and their claims arise under the same legal doctrines.

171. Adequacy of Representation, Fed. R. Civ. P. 23(a)(4): Plaintiffs will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiffs have no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiffs' counsel are competent and experienced in litigating complex class actions and data breach cases, and they intend to prosecute this actions vigorously.

172. Predominance, Fed. R. Civ. P. 23(b)(3): Defendants have engaged in a common course of conduct toward Plaintiffs and Class Members, in that all of Plaintiffs' and Class Members' data was stored on the same computer system and unlawfully accessed in the same way. The common issues arising from Defendants' conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

173. Superiority, Fed. R. Civ. P. 23(b)(3): A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendants. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

174. Manageability, Fed. R. Civ. P. 23(b)(3): The litigation of the claims brought herein is manageable. Defendants uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action. Adequate notice can be given to Class Members directly using information maintained in Defendants' records.

175. Conduct Generally Applicable to the Class**,** Fed. R. Civ. P. 23(b)(2): Further, Defendants have acted or refused to act on grounds generally applicable to

the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate. Unless a class-wide injunction is issued, Defendants may continue in its failure to properly secure the PII of Class Members, Defendants may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendants may continue to act unlawfully as set forth in this Complaint.

176. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. The particular issues include, but are not limited to:

(a) Whether Defendants owed a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

(b) Whether Defendants breached a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

(c) Whether Defendants failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

(d) Whether an implied contracts existed between Defendants on the one hand, and Plaintiffs and Class Members on the other, and the terms of those implied contracts;

(e) Whether Defendants breached the implied contracts;

(f) Whether Defendants adequately, and accurately informed Plaintiffs and Class Members that their PII had been compromised;

(g) Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

(h) Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiffs and Class Members; and

(i) Whether Class Members are entitled to actual damages, statutory damages, nominal damages, injunctive relief, and/or punitive damages as a result of Defendants wrongful conduct.

COUNT I
<u>NEGLIGENCE</u>
(On Behalf of Plaintiffs and the Class)

177. Plaintiffs repeat and re-allege paragraphs 1-176 as if fully set forth herein.

178. Plaintiffs bring this Count on behalf of themselves and the Class.

179. As a condition of receiving their mortgages or related services from Defendants or their partners or affiliates, Plaintiffs and the Class were obligated to provide and entrust them with certain PII, including their name, birthdate, address, loan number, Social Security number, and other information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

180. Plaintiffs and the Class provided and entrusted their PII to Defendants on the premise and with the understanding that Defendants would safeguard their information, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

181. By undertaking the duty to maintain and secure this data, sharing it and using it for commercial gain, Defendants had a duty of care to use reasonable means to secure and safeguard their systems and networks—and Plaintiffs and the Class Members' PII held within it—to prevent disclosure of the information, and to safeguard the information from cyber theft.

182. Defendants had full knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and the Class could and would suffer if the PII were wrongfully disclosed or obtained by unauthorized parties.

183. Defendants knew or reasonably should have known that their failure to exercise due care in the collecting, storing, and using of consumers' PII involved an unreasonable risk of harm to Plaintiffs and the Class, including harm that foreseeably could occur through the criminal acts of a third party.

184. Defendants had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendants' security protocols to ensure that Plaintiffs' and Class Members' information in their possession was adequately secured and protected.

185. Defendants also had a duty to exercise appropriate clearinghouse practices to remove former customers' or rejected loan applicants PII that they were no longer required to retain pursuant to regulations.

186. Defendants had a duty to have procedures in place to detect and prevent the improper access and misuse of Plaintiffs' and the Class's PII, and to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiffs and the Class.

187. Defendants' duty to use reasonable security measures arose as a result of the special relationship that existed between each Defendant and Plaintiffs and the Class. That special relationship arose because Plaintiffs and the Class entrusted Defendants with their confidential PII, a mandatory step in receiving services from Defendants. While this special relationship exists independent from any contract, it is recognized by Defendants' Privacy Policies, as well as applicable laws and regulations. Specifically, Defendants actively solicited and gathered PII as part of their businesses and were solely responsible for and in the position to ensure that their systems were sufficient to protect against the foreseeable risk of harm to Plaintiffs, Class and Subclass members from a resulting data breach.

188. Defendants were subject to an "independent duty," untethered to any contract between Defendants and Plaintiffs and the Class, to maintain adequate data security.

189. A breach of security, unauthorized access, and resulting injury to Plaintiffs and the Class was reasonably foreseeable, particularly in light of Defendants' inadequate security practices.

190. Defendants also had a common law duty to prevent foreseeable harm to others. Plaintiffs and the Class were the foreseeable and probable victims of Defendants' inadequate security practices and procedures. Defendants knew or should have known of the inherent risks in collecting and storing the PII of Plaintiffs and the Class, the critical importance of adequately safeguarding that PII, and the necessity of encrypting PII stored on Defendants' systems. It was foreseeable that Plaintiffs and Class members would be harmed by the failure to protect their personal information because hackers are known to routinely attempt to steal such information and use it for nefarious purposes.

191. Defendants' conduct created a foreseeable risk of harm to Plaintiffs and the Class. Defendants' wrongful conduct included, but was not limited to, their failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendants' misconduct also included their decision not to comply with industry standards for the safekeeping of Plaintiffs' and the Class's PII, including basic encryption techniques available to Defendants.

192. Plaintiffs and the Class had and have no ability to protect their PII that was in, and remains in, Defendants' possession.

193. Defendants were in a position to effectively protect against the harm suffered by Plaintiffs and the Class as a result of the Data Breach.

194. Defendants had and continue to have a duty to adequately disclose that the PII of Plaintiffs and the Class within Defendants' possession was compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiffs and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

195. Defendants have admitted that the PII of Plaintiffs and the Class was wrongfully accessed by unauthorized third persons as a result of the Data Breach.

196. Defendants, through their actions and inaction, unlawfully breached their duties to Plaintiffs and the Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII of Plaintiffs and the Class when the PII was within Defendants' possession or control.

197. Defendants improperly and inadequately safeguarded the PII of Plaintiffs and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

198. Defendants failed to heed industry warnings and alerts to provide adequate safeguards to protect their current and former customers' PII in the face of increased risk of theft.

199. Defendants, through their actions and/or omissions, unlawfully breached their duty to Plaintiffs and the Class by failing to have appropriate procedures in place to detect and prevent dissemination of their current and former customers' PII.

200. Defendants breached their duty to exercise appropriate clearinghouse practices by failing to remove consumers' PII they were no longer required to retain pursuant to regulations.

201. Defendants, through their actions and/or omissions, unlawfully breached their duty to adequately and timely disclose to Plaintiffs and the Class the existence and scope of the Data Breach.

202. But for Defendants' wrongful and negligent breach of duties owed to Plaintiffs and the Class, the PII of Plaintiffs and the Class would not have been compromised.

203. There is a close causal connection between (a) Defendants' failure to implement security measures to protect the PII of Plaintiffs and the Class and (b) the harm or risk of imminent harm suffered by Plaintiffs and the Class. Plaintiffs' and the Class's PII was accessed and exfiltrated as the direct and proximate result of Defendants' failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

204. As a direct and proximate result of Defendants' negligence, Plaintiffs and the Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity to control how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII for Plaintiffs' and Class Members' respective lifetimes; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the present and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and other identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the current and former customers' PII in their continued possession; and (viii) present and future costs in the form of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the compromise of PII as a result of the Data Breach for the remainder of the lives of Plaintiffs and the Class Members.

205. As a direct and proximate result of Defendants' negligence, Plaintiffs and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

206. Additionally, as a direct and proximate result of Defendants' negligence, Plaintiffs and the Class have suffered and will suffer the continued risks of exposure of their PII, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII in their continued possession.

207. As a direct and proximate result of Defendants' negligence, Plaintiffs are now at an increased risk of identity theft or fraud.

208. As a direct and proximate result of Defendants' negligence, Plaintiffs are entitled to and demand actual, consequential, and nominal damages and injunctive relief to be determined at trial.

COUNT II
INVASION OF PRIVACY – INTRUSION UPON SECLUSION
(On Behalf of Plaintiffs and the Class)

209. Plaintiffs repeat and re-allege paragraphs 1-176 as if fully set forth herein.

210. Plaintiffs bring this Count on behalf of themselves and the Class.

211. Defendants intentionally intruded into Plaintiffs' and Class Members'

seclusion by failing to keep their PII secure.

212. By failing to keep Plaintiffs' and Class Members' PII secure, and allowing for access and disclosing of the PII to unauthorized parties for unauthorized use, Defendants unlawfully invaded Plaintiffs' and Class Members' privacy right to seclusion by, *inter alia*:

(a) intruding into their private affairs in a manner that would be highly offensive to a reasonable persons;

(b) invading their privacy by improperly using their PII properly obtained for a specific purpose for another purpose, or disclosing it to unauthorized persons;

(c) failing to adequately secure their PII from disclosure to unauthorized persons; and

(d) enabling the disclosure of their PII without consent.

213. The PII that was publicized during the Data Breach was highly sensitive, private, and confidential, as it included private financial, employment, and personal information.

214. As a direct and proximate result of Defendants' intrusion upon seclusion, Plaintiffs and Class Members suffered injury and sustained actual losses and damages as alleged herein. Plaintiffs and Class Members alternatively seek an award of nominal damages.

COUNT III
<u>UNJUST ENRICHMENT</u>
(On Behalf of Plaintiffs and the Class)

215. Plaintiffs repeat and re-allege paragraphs 1-176 as if fully set forth herein.

216. Plaintiffs bring this Count on behalf of themselves and the Class.

217. For years and continuing to today, Defendants' business model has depended upon it being entrusted with customers' PII. Trust and confidence are critical and central to the services provided by Defendants in the residential financing industry. Unbeknownst to Plaintiffs and absent Class Members, however, Defendants did not secure, safeguard, or protect its customers' and employees' data and employed deficient security procedures and protocols to prevent unauthorized access to customers' PII. Defendants' deficiencies described herein were contrary to their security messaging.

218. Plaintiffs and Class Members received services from Defendants, and Defendants were provided with, and allowed to collect and store, their PII on the mistaken belief that Defendants complied with their duties to safeguard and protect its customers' and employees' PII. Upon information and belief, putting their short-term profit ahead of safeguarding PII, and unbeknownst to Plaintiffs and absent Class Members, Defendants knowingly sacrificed data security to save money.

219. Upon information and belief, Defendants knew that the manner in which they maintained and transmitted customer PII violated industry standards and their fundamental duties to Plaintiffs and absent Class Members by neglecting well-

accepted security measures to ensure confidential information was not accessible to unauthorized access. Defendants had knowledge of methods for designing safeguards against unauthorized access and eliminating the threat of exploit, but it did not use such methods.

220. Defendants had within their exclusive knowledge, and never disclosed, that they had failed to safeguard and protect Plaintiffs' and absent Class Members' PII. This information was not available to Plaintiffs, absent Class Members, or the public at large.

221. Defendants also knew that Plaintiffs and Class Members expected security against known risks and that they were required to adhere to state and federal standards for the protection of confidential personally identifying, financial, and other personal information.

222. Plaintiffs and absent Class Members did not expect that Defendants would knowingly insecurely maintain and hold their PII when that data was no longer needed to facilitate a business transaction or other legitimate business reason. Likewise, Plaintiffs and absent Class Members did not know or expect that Defendants would employ substantially deficient data security systems and fail to undertake any required monitoring or supervision of the entrusted PII.

223. Had Plaintiffs and absent Class Members known about Defendants' efforts to deficiencies and efforts to hide their ineffective and substandard data

security systems, Plaintiffs and absent Class Members would not have entered business dealings with Defendants.

224. By withholding the facts concerning the defective security and protection of customer PII, Defendants put their own interests ahead of the very customers who placed their trust and confidence in Defendants, and benefitted themselves to the detriment of Plaintiffs and absent Class Members.

225. As a result of its conduct as alleged herein, Defendants sold more services than it otherwise would have, and was able to charge Plaintiffs and Class Members more for mortgage services than it otherwise could have. Defendants were unjustly enriched by charging for and collecting for those services that it would not have obtained to the detriment of Plaintiffs and absent Class Members.

226. It would be inequitable, unfair, and unjust for Defendants to retain these wrongfully obtained fees and benefits. Defendants' retention of wrongfully obtained monies would violate fundamental principles of justice, equity, and good conscience.

227. Defendants' unfair and deceptive conduct to not disclose those defects have, among other things, caused Plaintiffs and Class Members to enter a business arrangement that was deceptive and dangerous to their identities.

228. As a result, Plaintiffs paid for services that they would not have paid for had Defendants disclosed the inadequacy of its data security practices.

229. Plaintiffs and each Member of the proposed Class are each entitled to restitution and non-restitutionary disgorgement in the amount by which Defendants were unjustly enriched, to be determined at trial.

COUNT IV
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Class)

230. Plaintiffs repeat and re-allege paragraphs 1-176 as if fully set forth herein.

231. Plaintiffs bring this Count on behalf of themselves and the Class.

232. KeyBank solicited and invited prospective customers to provide their PII as part of its regular business practices. Plaintiffs and the Class Members provided KeyBank with heir PII, directly or indirectly, including their names, birthdates, addresses, loan numbers, Social Security numbers, and information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

233. OSC acquired and maintained the PII of Plaintiffs and the Class that it received from KeyBank. The PII included names, birthdates, addresses, loan numbers, Social Security numbers, and information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

234. When Plaintiffs and Class Members paid money and provided their PII to KeyBank, either directly or indirectly, in exchange for goods or services, they entered into implied contracts with KeyBank and its vendors, including OSC, pursuant to which KeyBank and OSC agreed to safeguard and protect such information and to timely and accurately notify them if their data had been breached and compromised.

235. KeyBank solicited and invited prospective customers to provide their PII as part of its regular business practices. As a condition of receiving services, KeyBank required Plaintiffs and Class Members to provide their PII, including names, Social Security numbers, driver's license numbers, addresses, dates of birth, email addresses, financial account numbers, and payment information.

236. Pursuant to FTC guidelines and standard practice in the financial industry, KeyBank was obligated to take reasonable steps to maintain the security of Plaintiffs' and Class Members' PII. As a result, by requesting that Plaintiffs and Class Members provide their PII as part of their doing business with KeyBank, KeyBank implicitly promised to adhere to these industry standards. By entering into a third-party vendor agreement with KeyBank, OSC implicitly agreed to adhere to those same FTC guidelines and standard practices of the financial industry.

237. Plaintiffs and Class Members each accepted KeyBank's offers and provided their PII to KeyBank, and by extension OSC. In entering into such implied contracts, Plaintiffs and the Class reasonably believed that KeyBank's data security practices and policies, and the practices of its third-party vendors, including OSC, were reasonable and consistent with industry standards, and that KeyBank and OSC would use part of the fees received from Plaintiffs and the Class to pay for adequate and reasonable data security practices to safeguard the PII.

238. Plaintiffs and Class Members accepted KeyBank offers and provided their PII to KeyBank, who then entrusted the PII to OSC. Defendants accepted the PII, and there was a meeting of the minds that Defendant would secure, protect, and keep the PII confidential.

239. Plaintiffs fully performed their obligations under the implied contracts with Defendants.

240. Plaintiffs would not have entered into transactions with Defendants if Plaintiffs had known that Defendants would not protect their PII.

241. Plaintiffs and the Class would not have provided and entrusted their PII to KeyBank in the absence of the implied contract between them and KeyBank to keep the information secure.

242. Plaintiffs and the Class fully performed their obligations under the implied contracts with Defendants.

243. Defendants breached its implied contracts with Plaintiffs and the Class by failing to safeguard and protect their PII and by failing to provide timely and accurate notice that their PII was compromised as a result of the Data Breach.

244. As a direct and proximate result of Defendants breaches of their implied contracts, Plaintiffs and the Class sustained actual losses and damages as described herein.

COUNT V
<u>Violation of the Washington State Consumer Protection Act</u>
RCW 19.86.010 et seq.
(On Behalf of Plaintiff Patrick Reddy and the Washington Subclass)

245. Plaintiff Patrick Reddy ("Plaintiff," for purposes of this Count) repeats and re-alleges paragraphs 1-135 and 151-176 as if fully set forth herein.

246. Plaintiff brings this claim on behalf of himself of the Washington Subclass.

247. The Washington State Consumer Protection Act, RCW 19.86.020 (the "CPA") prohibits any "unfair or deceptive acts or practices" in the conduct of any trade or commerce as those terms are described by the CPA and relevant case law.

248. Defendants are a "person" as described in RWC 19.86.010(1).

249. Defendants engages in "trade" and "commerce" as described in RWC 19.86.010(2) in that they engage in the sale of services and commerce directly and indirectly affecting the people of the State of Washington.

250. By virtue of the above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Defendants engaged in unlawful, unfair and fraudulent practices within the meaning, and in violation of, the CPA, in that Defendants' practices were injurious to the public interest because they injured other persons, had the capacity to injure other persons, and have the capacity to injure other persons.

251. In the course of conducting their business, Defendants committed "unfair or deceptive acts or practices" by, inter alia, knowingly failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff's and Washington Subclass Members' PII, and violating the common law alleged herein in the process. Plaintiff and Washington Subclass Members reserve the right to allege other violations of law by Defendants constituting other unlawful business acts or practices. As described above, Defendants' wrongful actions, inaction, omissions, and want of ordinary care are ongoing and continue to this date.

252. Defendants also violated the CPA by failing to timely notify and concealing from Plaintiff and Washington Subclass Members regarding the unauthorized release and disclosure of their PII. If Plaintiff and Washington Subclass Members had been notified in an appropriate fashion, and had the information not

been hidden from them, they could have taken precautions to safeguard and protect their PII and identities.

253. Defendants' above-described wrongful actions, inaction, omissions, want of ordinary care, misrepresentations, practices, and non-disclosures also constitute "unfair or deceptive acts or practices" in violation of the CPA in that Defendants' wrongful conduct is substantially injurious to other persons, had the capacity to injure other persons, and has the capacity to injure other persons.

254. The gravity of Defendants' wrongful conduct outweighs any alleged benefits attributable to such conduct. There were reasonably available alternatives to further Defendants' legitimate business interests other than engaging in the above-described wrongful conduct.

255. As a direct and proximate result of Defendants' above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach and their violations of the CPA, Plaintiff and Washington Subclass Members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, inter alia, (1) an imminent, immediate and the continuing increased risk of identity theft, identity fraud and medical fraud—risks justifying expenditures for protective and remedial services for which he or she is entitled to compensation; (2) invasion of privacy; (3) breach of the confidentiality of his or her PII; (5) deprivation of the value of his or her PII, for which there is a well-established national and international market; and/or (6) the financial and temporal cost of monitoring credit, monitoring financial accounts, and mitigating damages.

256. Unless restrained and enjoined, Defendants will continue to engage in the above-described wrongful conduct and more data breaches will occur. Plaintiff, therefore, on behalf of himself, Class Members, and the general public, also seeks restitution and an injunction prohibiting Defendants from continuing such wrongful conduct, and requiring Defendants to modify their corporate culture and design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures protocols, and software and hardware systems to safeguard and protect the PII entrusted to it.

257. Plaintiff, on behalf of himself and the Class Members, also seeks to recover actual damages sustained by each class member together with the costs of the suit, including reasonable attorney fees. In addition, Plaintiff, on behalf of himself and the Class Members, requests that this Court use its discretion, pursuant to RCW 19.86.090, to increase the damages award for each class member by three times the actual damages sustained not to exceed $25,000.00 per class member.

COUNT VI
VIOLATIONS OF NEW YORK GENERAL BUSINESS LAW,
N.Y. Gen. Bus. Law § 349, et seq.
(On behalf of Plaintiff Mariann Archer and the New York Subclass)

258. Plaintiff Mariann Archer ("Plaintiff," for purposes of this Count) repeats and re-alleges paragraphs 1-150 and 164-176 as if fully set forth herein.

259. Plaintiff brings this count on behalf of herself and the New York Subclass.

260. Defendants engaged in deceptive acts or practices in the conduct of their business, trade, and commerce or furnishing of services, in violation of N.Y. Gen. Bus. Law § 349, including:

(a) Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and New York:

(b) Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

(c) Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Class Members' PII, including by implementing and maintaining reasonable security measures;

(d) Failing to timely and adequately notify the Plaintiff and Class Members of the Data Breach;

(e) Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Class Members' PII; and

(f) Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' PII, including duties imposed by the FTC Act, and N.Y. Gen. Bus. Law § 899-aa.

261. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII.

262. Defendants acted intentionally, knowingly, and maliciously to violate New York's General Business Law, and recklessly disregarded Plaintiff's and New York Subclass members' rights.

263. As a direct and proximate result of Defendants' deceptive and unlawful acts and practices, Plaintiff and New York Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their PII.

264. Defendants' deceptive and unlawful acts and practices complained of herein affected the public interest and consumers at large.

265. The above deceptive and unlawful practices and acts by Defendants caused substantial injury to Plaintiff and New York Subclass members that they could not reasonably avoid.

266. Plaintiff and New York Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of $50 (whichever is greater), treble damages, injunctive relief, and attorney's fees and costs.

COUNT XXI
VIOLATIONS OF INFORMATION SECURITY BREACH AND NOTIFICATION ACT,
N.Y. Gen. Bus. Law § 899-aa
(On behalf of Plaintiff Mariann Archer and the New York Subclass)

267. Plaintiff Mariann Archer ("Plaintiff," for purposes of this Count) repeats and re-alleges paragraphs 1-150 and 164-176 as if fully set forth herein.

268. Plaintiff brings this count on behalf of herself and the New York Subclass.

269. Defendants are each a business that owns or licenses computerized data that includes Personal Information as defined by N.Y. Gen. Bus. Law § 899-aa(1)(a). Defendants also maintain computerized data that includes PII which Defendants do not own. Accordingly, they are subject to N.Y. Gen. Bus. Law §§ 899- aa(2) and (3).

270. Plaintiff's and New York Subclass members' private information (e.g. Social Security numbers) includes PII covered by N.Y. Gen. Bus. Law § 899-aa(1)(b).

271. Defendants are required to give immediate notice of a breach of security of a data system to owners of PII which Defendants do not own, including Plaintiff and New York Subclass members, pursuant to N.Y. Gen. Bus. Law § 899-aa(3).

272. Defendants are required to accurately notify Plaintiff and New York Subclass members if it discovers a security breach or receives notice of a security breach which may have compromised PII which Defendants own or license, in the most expedient time possible and without unreasonable delay under N.Y. Gen. Bus. Law § 899-aa(2).

273. By failing to disclose the Data Breach in a timely and accurate manner, Defendants violated N.Y. Gen. Bus. Law §§ 899-aa(2) and (3).

274. As a direct and proximate result of Defendants violations of N.Y. Gen. Bus. Law §§ 899-aa(2) and (3), Plaintiff and New York Subclass members suffered damages, as described above.

275. Plaintiff and New York Subclass members seek relief under N.Y. Gen. Bus. Law § 899-aa(6)(b), including actual damages and injunctive relief.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for judgment as follows:

A. For an Order certifying the Class, or alternatively, the New York and Washington Classes, and appointing Plaintiffs and their counsel to represent the certified Class and/or Classes;

B. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and the Class Members' PII, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiffs and Class Members;

C. For injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order:

i. prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendants to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendants to delete, destroy, and purge the personal identifying information of Plaintiffs and Class Members unless

Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

iv. requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the Plaintiffs' and Class Members' PII;

v. prohibiting Defendants from maintaining Plaintiffs' and Class Members' PII on a cloud-based database;

vi. requiring Defendants to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendants to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendants to segment data by, among other things, creating firewalls and access controls so that if one area of Defendants' network is compromised, hackers cannot gain access to other portions of Defendants' systems;

x. requiring Defendants to conduct regular database scanning and securing checks;

xi. requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling PII, as well as protecting the PII of Plaintiffs and Class Members;

xii. requiring Defendants to conduct internal training and education routinely and continually, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendants to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with

Defendants' policies, programs, and systems for protecting PII;

xiv. requiring Defendants to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendants' information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendants to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendants to implement logging and monitoring programs sufficient to track traffic to and from Defendants servers; and

xvii. for a period of ten years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendants' compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with

compliance of the Court's final judgment.

D. For an award of damages, including a sum of money sufficient to provide to Plaintiffs and Class Members identity theft protection services for their respective lifetimes.

E. For an award of damages, including actual, statutory, nominal, and consequential damages, as allowed by law in an amount to be determined;

F. For an award of punitive damages;

G. For an award of attorneys' fees, costs, and litigation expenses pursuant to O.C.G.A. Section 13-6-11 and as otherwise allowed by law;

H. For prejudgment interest on all amounts awarded; and

H. Such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMAND

A jury trial is demanded by Plaintiffs and the putative Class Members as to all issues so triable.

September 20, 2022

Respectfully Submitted,

/s/ MaryBeth V. Gibson
MaryBeth V. Gibson
Georgia Bar No. 725843
THE FINLEY FIRM, P.C.
3535 Piedmont Rd.
Building 14, Suite 230

Atlanta, GA 30305
Phone: (404) 978-6971
Fax: (404) 320-9978
mgibson@thefinleyfirm.com

Terence R. Coates, Esq.*
Justin C. Walker, Esq. *
MARKOVITS, STOCK & DEMARCO, LLC
119 E. Court Street, Suite 530
Cincinnati, OH 45202
Phone: (513) 651-3700
Fax: (513) 665-0219
tcoates@msdlegal.com
jwalker@msdlegal.com

M. Anderson Berry, Esq.*
Clayeo C. Arnold, APLC
865 Howe Avenue
Sacramento, CA 95825
Phone: (916) 239-4778
Fax: (916) 924-1829
aberry@justice4you.com

*pro hac vice forthcoming

Attorneys for Plaintiff and the Proposed Class

CERTIFICATE OF COMPLIANCE

I certify that the foregoing pleading has been prepared with Times New Roman, 14-point font, in compliance with L.R. 5.1B.

/s/ MaryBeth V. Gibson
MARYBETH V. GIBSON